

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-195269

(43)Date of publication of application : 21.07.1999

(51)Int.Cl.

G11B 20/10
G09C 1/00
G09C 1/00
H04L 9/16
// G06F 17/60

(21)Application number : 09-369395

(71)Applicant : VICTOR CO OF JAPAN LTD

(22)Date of filing : 26.12.1997

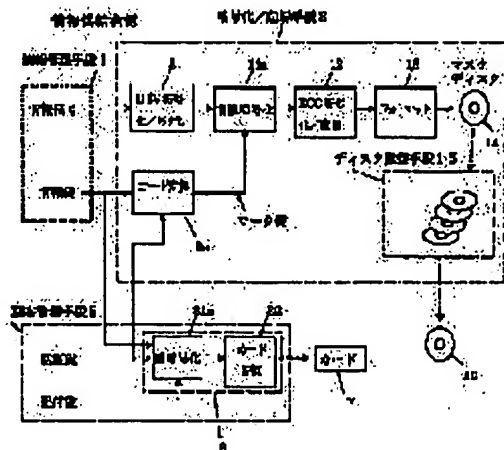
(72)Inventor : HIRATA ATSUMI
MACHIDA TOYOTAKA
HIROTA AKIRA

(54) INFORMATION CIPHERING METHOD, INFORMATION DECIPHERING METHOD, INFORMATION CIPHERING DEVICE, INFORMATION DECIPHERING DEVICE AND INFORMATION RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information ciphering method by which a ciphering and a deciphering are relatively simply and inexpensively enabled and the estimation of a deciphering key is made difficult.

SOLUTION: An information control means 1 accumulates information key codes peculiar to digital information and information signals. A customer control means 5 accumulates customer peculiar certifying keys and reproducing device peculiar distribution keys. Then, a code conversion means 9a converts the information key codes and generates work key codes. An information ciphering means 11a generates ciphering key codes from the work key codes and the sector numbers outputted from the means 9a. Then, the sectored digital information data are ciphered by using the ciphered key codes.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

31181 5020444 W000

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-195269

(43) 公開日 平成11年(1999) 7月21日

(51) Int. Cl. ⁵	識別記号	F I
G 1 1 B 20/10		G 1 1 B 20/10 H
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00 6 1 0 Z
	6 6 0	6 6 0 D
H 0 4 L 9/16		H 0 4 L 9/00 6 4 3
// G 0 6 F 17/60		G 0 6 F 15/21 3 4 0 Z
審査請求 未請求 請求項の数 9 F D (全 9 頁)		

(21) 出願番号 特願平9-369395

(22) 出願日 平成9年(1997)12月26日

(71) 出願人 000004329

日本ビクター株式会社

神奈川県横浜市神奈川区守屋町3丁目12番地

(72) 発明者 平田 渥美

神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(72) 発明者 町田 豊隆

千葉県柏市篠簞田1135-1 サルビア703

(72) 発明者 廣田 昭

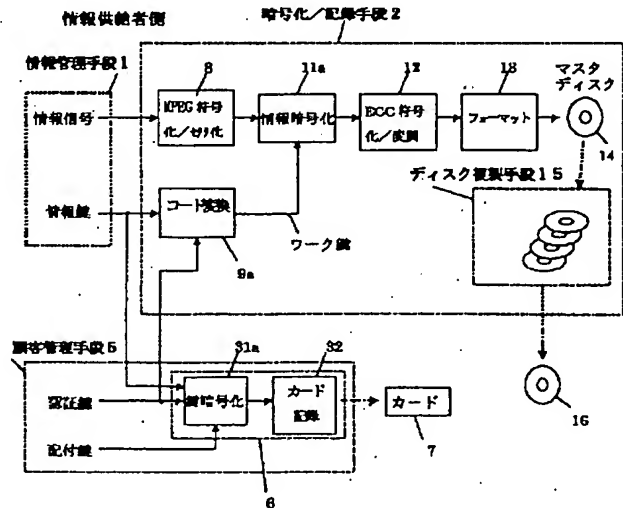
神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

(54) 【発明の名称】 情報暗号化方法、情報復号方法、情報暗号化装置、情報復号装置及び情報記録媒体

(57) 【要約】

【課題】 比較的簡単で安価に暗号化及び復号が可能で、しかも復号鍵の推定が困難な情報暗号化方法がなかった。

【解決手段】 情報管理手段1は、デジタル情報に固有の情報鍵コードと情報信号とを蓄積している。また、顧客管理手段5は、顧客固有の認証鍵と再生装置固有の配付鍵を蓄積している。そして、コード変換手段9aにより情報鍵コードをコード変換してワーク鍵コードを生成する。さらに、情報暗号化手段11aでは、コード変換手段9aより出力されるワーク鍵コードとセクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化されたデジタル情報データを暗号化する。



【特許請求の範囲】

【請求項1】 デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化方法において、
前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生成し、
このワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、
この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化することを特徴とする情報暗号化方法。

【請求項2】 複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号方法において、
前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号し、
この情報鍵コードをコード変換してワーク鍵コードを生成し、
このワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、
この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号することを特徴とする情報復号方法。

【請求項3】 前記ワーク鍵コードは、
情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成し、
前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成し、
前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成し、
前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更して生成されることを特徴とする請求項1記載の情報暗号化方法又は請求項2記載の情報復号方法。

【請求項4】 前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする請求項1記載の情報暗号化方法又は請求項2記載の情報復号方法。

【請求項5】 デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化装置において、

前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生ずるコード変換手段と、
このコード変換手段より出力されるワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化する情報暗号化手段とを有することを特徴とする情報暗号化装置。

【請求項6】 複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号装置において、
前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号する鍵復号手段と、

この鍵復号手段にて復号された情報鍵コードをコード変換してワーク鍵コードを生成するコード変換手段と、
このコード変換手段にて生成されたワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号する情報復号化手段とを有することを特徴とする情報復号装置。

【請求項7】 前記コード変換手段は、
情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成するビット列分割／加算手段と、
前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成する加算手段と、
前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成するビットローテーション手段と、
前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更してワーク鍵コード得ることを特徴とする請求項5記載の情報暗号化装置又は請求項6記載の情報復号装置。

【請求項8】 前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする請求項5記載の情報暗号化装置又は請求項6記載の情報復号装置。

【請求項9】 複数のセクタに分割されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている情報記録媒体であって、
前記デジタル情報データは、前記デジタル情報に固有の情報鍵コードをコード変換したワーク鍵コードと前記セクタ番号とから生成される暗号化鍵コードを使用して暗

号化されていることを特徴とする情報記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報の暗号化／復号方法に係り、特に、映像信号、音声信号、データ信号等の情報をセクタ化して、ディスク等の情報記録媒体に記録／再生を行う場合に用いて好適な情報暗号化方法、情報復号方法、情報暗号化装置、情報復号装置及び情報記録媒体に関するものである。

【0002】

【従来の技術】従来より、所定の記録媒体に情報を暗号化して記録する場合、所定の暗号化鍵を用いて情報を暗号化して所定の記録媒体に記録すると同時に、暗号化された情報を復号するための復号鍵（あるいは復号鍵に対応する情報）を、同一記録媒体に記録している。この場合、復号鍵（あるいは復号鍵に対応する情報）は、記録媒体の所定の連続した領域に連続して記録、あるいは、連続しない複数の領域に分散して記録している。

【0003】復号は、記録媒体から再生して得た復号鍵、あるいは復号鍵に対応する情報を基に生成した復号鍵を用いて、同じ記録媒体から再生される暗号化された情報を復号していた。

【0004】また、暗号化は、少なくとも一つの情報については一つの暗号鍵を用いて暗号化している。例えば、60分間長の映画の情報を暗号化する場合、60分間全編に亘って同一の暗号鍵を用いて暗号化していた。

【0005】

【発明が解決しようとする課題】従来は、暗号化された情報と、その暗号化された情報を復号するために用いる復号鍵（あるいは復号鍵に対応する情報）とが、同一の記録媒体に記録されており、また一つの情報全体に亘って同一暗号鍵を用いて暗号化しているため、復号鍵を推定され易いという課題があった。また、情報記録媒体内に、復号鍵（あるいは復号鍵に対応する情報）を記録しているので、情報記録媒体内にそのための領域を確保する必要があり、その分、本来の情報を記録する領域が減少していた。

【0006】なお、比較的簡単で且つ効果的な暗号化／復号化方法として、共通鍵方式によるPN加算方式がある。この方式は、擬似ランダム加算方式とも呼ばれ、M系列符号発生器を利用して情報を暗号化するものである。しかし、この方式でも、内容に一定の規則性がある複数の復号鍵を準備し、それらをつづつ用いて、暗号化された情報の復号を試み、個々の復号結果と、復号鍵間の規則性との相関を解析することによって、その暗号化された情報に用いられた暗号鍵及びその復号鍵を推定することが比較的容易に可能である。したがって、暗号化された情報を不正に解読される危険性があった。

【0007】また、これらの問題を解決する方法として、例えば、ブロック暗号化方式、公開鍵方式等種々提

案されているが、いずれも複雑で復号処理に時間が掛かるので、映画や音楽などのリアルタイムで再生する必要のある情報の暗号化処理には不向きであったり、高価な装置が必要になったりする等の問題があった。

【0008】そこで本発明は、比較的簡単で安価に暗号化及び復号が可能で、しかも復号鍵の推定が困難な情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体を提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するための手段として、以下の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体を提供する。

【0010】1. デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化方法において、前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生成し、このワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化することを特徴とする情報暗号化方法。

【0011】2. 複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号方法において、前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号し、この情報鍵コードをコード変換してワーク鍵コードを生成し、このワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号することを特徴とする情報復号方法。

【0012】3. 前記ワーク鍵コードは、情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成し、前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成し、前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成し、前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更して生成されることを特徴とする上記1記載の情報暗号化方法又は上記2記載の情報復号方法。

【0013】4. 前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算

した余り値を使用して発生した擬似ランダムコード列であることを特徴とする上記1記載の情報暗号化方法又は上記2記載の情報復号方法。

【0014】5. デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化装置において、前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生ずるコード変換手段と、このコード変換手段より出力されるワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化する情報暗号化手段とを有することを特徴とする情報暗号化装置。

【0015】6. 複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号装置において、前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号する鍵復号手段と、この鍵復号手段にて復号された情報鍵コードをコード変換してワーク鍵コードを生成するコード変換手段と、このコード変換手段にて生成されたワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号する情報復号化手段とを有することを特徴とする情報復号装置。

【0016】7. 前記コード変換手段は、情報鍵コードを等ビット数の複数の部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成するビット列分割/加算手段と、前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成する加算手段と、前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成するビットローテーション手段と、前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更してワーク鍵コードを得ることを特徴とする上記5記載の情報暗号化装置又は上記6記載の情報復号装置。

【0017】8. 前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする上記5記載の情報暗号化装置又は上記6記載の情報復号装置。

【0018】9. 複数のセクタに分割されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている情報記録媒体であって、前記デジタル情報データは、前記デジタル情報に固有の情報鍵コードをコード

変換したワーク鍵コードと前記セクタ番号とから生成される暗号化鍵コードを使用して暗号化されていることを特徴とする情報記録媒体。

【0019】

【発明の実施の形態】本発明の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体の詳細な説明をするのに先だって、先ず本発明の利用分野である情報供給システムの概要について図1を用いて説明する。

【0020】同図において、情報の供給者は、記録媒体3に記録して販売等に供する情報（コンテンツ）の管理や情報に固有の情報鍵の生成管理等を行う情報管理手段1と、顧客情報の管理、配付鍵や認証鍵の生成管理、課金管理等を行う顧客管理手段5とを有している。

【0021】そして、所定の情報を所定の顧客に供給するに当たっては、まず、情報供給者は、暗号化/記録手段2において、顧客が所望する情報を、その情報に固有の情報鍵及び顧客に情報の取得を認可する認証鍵を用いて暗号化し、所定の情報記録媒体3に記録して顧客に供給する一方で、暗号化された情報を復号するために用いる復号鍵を生成するための情報として、情報鍵、認証鍵等（あるいは、それらに対応した情報等）を配付鍵を用いて暗号化し、カード発行手段6によってカード7に記録して、顧客に配付する。顧客は受け取った情報記録媒体3及びカード7を再生/復号化手段4に装着して、所定の情報を取得する。なお、認証鍵は、顧客あるいは顧客が属するグループ等に固有の予め付与した情報であり、また、配付鍵は顧客が使用する情報再生/復号装置に固有の予め付与した情報である。

【0022】このような情報供給システムにおいて本発明は、この暗号化および復号化に関して新たな提案を行うものである。すなわち、本発明は、デジタル情報を複数のセクタに分割し、各セクタに付与したセクタ番号及び情報に固有の情報鍵を基に生成した暗号鍵を用いて、各セクタ毎に情報を暗号化し、その暗号化したデジタル情報データを記録媒体に記録するものである。

【0023】ここで、セクタ番号は各セクタに固有の番号であるため、各セクタはそれぞれセクタに固有の暗号鍵を用いて暗号化されることになる。すなわち、情報は、頻繁に（下記に詳述する実施例では約0.003秒間隔で）更新される暗号鍵を用いて暗号化される。この様に短い間隔で暗号鍵が更新されるため、暗号化された情報から、それに用いられた暗号鍵及びその復号鍵を推定することは極めて困難となる。

【0024】また、暗号化及び復号化に当たって、情報鍵コードを別のコードに変換し、その変換されたワーク鍵コードを用いて暗号鍵及び復号鍵を生成している。これにより、互いに規則性のある複数の情報鍵を準備して復号鍵の推定を試みようとしても、このコード変換によって、規則性が崩れるため復号鍵の推定が困難とな

る。

【0025】以下、本発明の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体の一実施例として、暗号化された情報を記録する記録媒体としてDVD(Digital Versatile Disk)を用いた場合について説明する。なお、本発明で使用する情報記録媒体としては、DVDに限らず、他の磁気テープ、磁気ディスク等も有効である。

【0026】

【実施例】図2は、本発明の暗号化装置で情報供給側の構成例を示すブロック図である。同図において、情報管理手段1は、販売等に供する情報(映像情報、音声情報、データ情報等のコンテンツ情報、以下コンテンツ情報ともいう)を在庫として保有するとともにそれを管理し、必要に応じて情報信号を暗号化して記録媒体に記録するために、暗号化/記録手段2に供給するものである。また、情報信号を暗号化/記録手段2に供給する際には、そのコンテンツ情報に固有の情報である情報鍵コードを、暗号化/記録手段2及び顧客管理手段5に供給する。

【0027】顧客管理手段5は、配付鍵、認証鍵等の管理を行い、コンテンツ情報を顧客に供給する際に、認証鍵コードを暗号化/記録手段2に供給する。また、配付鍵コードを用いて、情報鍵コード及び認証鍵コードを暗号化し、カード記録手段32に出力してカード状情報記録媒体(以下、カードと記す)7に記録して、顧客(ユーザ、情報利用者)に配付する。なお、認証鍵は、ユーザあるいはユーザが属するグループ等を識別するための固有の情報(例えば会員番号や顧客管理番号)であり、また、配付鍵はユーザが使用する情報再生/復号手段4を識別するための固有の情報(例えば装置の製造番号等の識別番号)である。

【0028】情報管理手段1から暗号化/記録手段2に供給された情報信号は、まず、MPEG符号化/セクタ化手段8に入力される。MPEG符号化/セクタ化手段8は、入力された情報信号をMPEG方式による圧縮符号化を行ってデジタル情報データを生成し、更に、このデジタル情報データを2048バイトから成る複数のセクタに分割する。

【0029】その後、DVDフォーマットに合わせるために、各セクタにセクタ管理情報、セクタ番号等を付加して、2064バイトで構成されるデータセクタを構築し、順次、暗号化手段11aに供給する。

【0030】このMPEG符号化/セクタ化手段8で構築されるデータセクタの構造を図4に示す。図4(b)に示す1データセクタは、IDデータ(4バイト)、IDデータのエラー検出符号であるIED(2バイト)、メインデータ(2048バイト)及びメインデータのエラー検出符号であるEDC(4バイト)で構成されている。更に、このIDデータは図4(a)に示すように、セクタ情報データ(1バイト)と

セクタ番号(3バイト)とで構成される。なお、セクタ化されたデジタル情報データは、上記のメインデータ領域に収納される。また、セクタ番号は、各データセクタの序列を示し、通常は最初のセクタからの通し番号である。

【0031】また、情報管理手段1から暗号化/記録手段2に供給された情報鍵コードは、コード変換器9aに入力される。また、顧客管理手段5から暗号化/記録手段2に供給された認証鍵コードも、コード変換器9aに入力される。そして、コード変換器9aは、入力された情報鍵コードと認証鍵コードとの間で後述する所定の演算及びコード変換処理を行ない、その結果得たワーク鍵コードを暗号手段11aに供給する。

【0032】ここでは、情報鍵コードを暗号鍵生成要素の一つとして使用しているが、情報管理手段1から供給された情報鍵コードを、別のコードに変換することによって、暗号鍵および復号鍵の秘匿性を高めている。そして、図6にコード変換器9aの構成例を示し、図7にその演算及びコード変換処理の手順を示す。情報鍵コードは、下述の手順でコード変換されてワーク鍵コードとして出力される。

【0033】入力される情報鍵コードは、ビット列分割/加算器27に供給される。ビット列分割/加算器27は、供給される入力コード(情報鍵コード)を任意の等ビット長からなる複数の部分ビット列D0, D1, ..., D9に分割する(図7(a))。そして、一つの部分ビット列(実施例ではD4であるが、これに限らない)を、残りの各部分ビット列に、個別に排他的論理加算して新たな部分ビット列(第一のビット列)E0, E1, ..., E9を得る。この時、D4同士の排他的論理和は採らずにE4 = D4とする。そして、これらの部分ビット列E0, E1, ..., E9を結合して新たなビット列を得て、加算器30に出力する(図7(b))。

【0034】加算器30は、ビット列分割/加算器27から供給される新たなビット列に対して、顧客管理手段5から供給される情報鍵コードと等ビット数の認証鍵コード(図7(c), 第二のビット列)を排他的論理加算し、得られたビット列を任意の等ビット長の複数の部分ビット列(第三のビット列)F0, F1, ..., F4に分割してビットローテーション器28に出力する(図7(d))。

【0035】ビットローテーション器28は、供給される部分ビット列F0, F1, ..., F4を分割された各部分ビット列単位(F0内、F1内、...)で、所定のビット数だけ右にローテートし(図7(e))、部分ビット列G0, G1, ..., G4(第四のビット列)を得る(図7(f))。この部分ビット列G0, G1, ..., G4は、ビット列転置器29に供給され、部分ビット列G0, G1, ..., G4の配列順序を任意に変更する。そして、その結果得たビット列をワーク鍵コードとして情報暗号化手段11aに出力する(図7(g))。

【0036】以上説明したコード変換器9aは、入力情

報鍵コードを一意的ワーク鍵コードに変換し、入力情報鍵コードが規則的に変化しても、それに対応してワーク鍵コードはランダムに変化するという特徴を有して居るので、この様なワーク鍵コードを用いて暗号化された情報から、それを復号するための復号鍵を推測することは極めて困難である。

【0037】なお、上記した各部分ビット列のビット長や分割数などは任意であるが、後述する再生／復号手段4で使用するコード変換手段9bと同じビット長及び分割数の部分ビット列とする必要がある。

【0038】情報暗号化手段11aは、コード変換器9aから供給されたワーク鍵コードに基づいて、MPEG符号化／セクタ化手段8から供給されたセクタデータを暗号化し、暗号化されたセクタデータをECC符号化／変調手段12に供給する。

【0039】ここで、情報暗号化手段11aの構成例を図5に示し、図4を参照しながらその動作について説明する。同図において、セクタデータは、入力ビット列として信号分割器22及びセクタ解読器23に入力される。また、ワーク鍵コードは除算器21に入力される。

【0040】セクタ解読器23は、セクタデータ内のIDデータを検出解読して、入力ビット列がメインデータ領域期間中である場合には、分割制御信号(図4(d))を信号分割器22に供給する。また、セクタ番号を抽出して、除算器21に出力する。さらに、各セクタの開始時点(メインデータ領域期間となる前)に、初期化制御信号(図4(c))をM列符号発生器24に供給する。

【0041】信号分割器22は、セクタ解読器23から供給される分割制御信号に応じて、セクタデータ内のメインデータを加算器26に供給すると共に、それ以外のデータを信号結合器25に供給する。

【0042】一方、除算器21は、セクタ解読器23から供給されるセクタ番号でワーク鍵コードを除算し、その結果得た余り値を初期値としてM系列符号発生器24に供給する。M系列符号発生器24は、セクタ解読器23から初期化制御信号が供給される度に、除算器21から供給される余り値を初期値として、疑似ランダムコード列(暗号化鍵コード)を発生し、加算器26に出力する。

【0043】加算器26は、信号分割器22から供給されるメインデータに、M系列符号発生器24から供給された疑似ランダムコードを排他論理加算することによってこれらを暗号化し、暗号化されたメインデータを信号結合器25に供給する。信号結合器25は、信号分割器22から供給されるIDデータ、IEDデータ及び著作権管理情報データと、加算器26から供給される暗号化されたメインデータとを結合して、暗号化されたセクタデータ(図4(e))を出力する。

【0044】ここで、IDデータ内のセクタ番号は、既述のごとく各セクタに固有の値である。したがって、M系

列符号発生器24は、各セクタ毎に、そのセクタに固有の値を初期値として疑似ランダムコード列を発生することになる。したがって、各セクタは、それぞれ異なるコード列で暗号化される。

【0045】また、1セクタは、既述のごとく2064バイト長であり、これは実時間再生で0.003秒間程度に相当する。すなわち、暗号化パターンが約0.003秒間隔で次々と変わることになる。したがって、情報記録媒体に記録された暗号化されたデータを再生して、そのデータパターンを解析して暗号鍵／復号鍵の解読を試みても、この様な短期間に解読することは困難である。

【0046】このようにして、情報暗号化手段11aは、各データセクタごとに暗号化されたセクタデータ列をECC符号化／変調器12に出力する。そして、情報暗号化器11aから出力された暗号化されたセクタデータ列は、公知のECC符号化／変調器12及び公知のフォーマット手段13により所定の処理を施されて、マスタディスク14に記録される。さらに、このマスタディスク14を基に、公知ディスク複製手段15を用いて、再生用ディスク16を複製してユーザに供給する。なお、多くの再生用ディスク16を必要としない場合には、マスタディスク14をユーザ供給用として使用しても良い。

【0047】さらに、情報提供者は、鍵暗号化手段31aにより、前述の情報鍵コード及び認証鍵コードを配付鍵コードを用いてそれぞれ暗号化し、カード記録手段32に供給してカード7に記録する。そして、このようにして配付鍵コードで暗号化された情報鍵コード及び認証鍵コードを記録したカード7をユーザに配付する。なお、鍵暗号化手段31aでの暗号化の手法やカード記録手段32及びカード7は特定のものである必要はなく、種々のものを使用することができる。

【0048】図3は、ユーザ側(情報利用者側)の構成例を示す図である。ユーザは、暗号化されたコンテンツ情報が記録された再生用ディスク(情報記録媒体)16と、暗号化された情報を復号するために必要な情報が記録されたカード7とを再生／復号手段4に装着して、暗号化されたコンテンツ情報を再生復号する。

【0049】同図に示す再生／復号手段4は、再生用ディスク16からデータを読み取ってデジタルデータを出力する公知の情報再生手段17と、データセクタに含まれるIEDやEDCを使用してエラー訂正をすると共に情報の復調を行う公知の復調／エラー訂正手段18と、情報復号化手段11bと、カード解読手段19と、配付鍵格納手段33と、鍵復号手段31bと、コード変換器9b及び公知のセクタ分解／MPEG復号手段20で構成されている。なお、コード変換器9b及び情報復号化手段11bは、それぞれ、既述の暗号化／記録手段2における、コード変換器9a及び情報暗号化手段11aと全く同一構成であり、同一動作及び同一機能を有している。

【0050】再生手段17は、再生用ディスク16から再生して得た再生情報を、復調／エラー訂正手段18に供給する。復調／エラー訂正手段18は、再生情報を復調してエラー訂正処理し、暗号化されたセクタデータを得て情報復号化手段11bに供給する。

【0051】一方、カード解読手段19は、カード7に記録されている暗号化された情報鍵コード及び暗号化された認証鍵コードを読み出し、これらを鍵復号手段31bに供給する。

【0052】鍵復号手段31bは、配付鍵格納手段33に格納されている配付鍵を用いて、暗号化されている情報鍵コードと認証鍵コードをそれぞれ復号して、情報鍵コードと認証鍵コードとをコード変換器9bに出力する。なお、配付鍵格納手段33に格納されている配付鍵は、再生／復号手段4に予め付与された装置の識別番号（例えば製造番号等）であり、顧客管理手段5に格納されている配付鍵と同一のものが使用される。なお、カード解読手段19及び鍵復号手段31bは種々のもの及び方法を使用することができる。

【0053】コード変換器9bの構成例を図6に示す。これは、既述の暗号化／記録手段2で用いたコード変換器9aと同一構成であるので、その動作の詳細な説明は省略する。そして、鍵復号手段31bから供給される認証鍵コードを用いて、同じく鍵復号手段31bから供給される情報鍵コードをワーク鍵コードに変換し、これを情報復号手段11bに出力する。

【0054】図5に情報復号化手段11bの構成例を示す。これは既述の情報暗号化手段11aと同一構成であり、その詳細な説明は省略するが、M系列符号発生手段24から出力される擬似ランダムコード列は復号鍵コードとして使用される。したがって、情報暗号化手段11aの場合は、入力ビット列として暗号化するべきセクタデータが入力され、出力ビット列として暗号化されたセクタデータが出力されるが、情報復号化手段11bでは、入力ビット列として暗号化されたセクタデータが入力され、出力ビット列として暗号化されたセクタデータを復号したセクタデータが出力される。ここで、ワーク鍵コードは、暗号化の場合と復号化の場合とで、同一コードある。したがって、暗号化されたセクタデータは、正確に元のセクタデータに復号される。

【0055】そして、復号されたセクタは、セクタ分離／MPEG復号手段20に出力され、元の情報信号にMPEG復号されて出力される。

【0056】

【発明の効果】本発明の情報暗号化方法、情報復号方法、情報暗号化装置及び情報復号装置情報記録媒体は、簡単な手段で強力な暗号化を行うことができる。

【0057】そして、本発明の情報記録媒体は、暗号鍵／復号鍵に関する情報を記録する必要がないので、そのための記録領域を確保する必要なく、情報の記録領域を

効率よく使用することができるという効果がある。

【図面の簡単な説明】

【図1】情報供給システムの一例を示す構成図である。

【図2】本発明の情報暗号化装置の一実施例を示す構成図である。

【図3】本発明の情報復号装置の一実施例を示す構成図である。

【図4】本発明の情報記録媒体に記録する情報のセクタ構造の例を示す図である。

【図5】情報暗号化手段及び情報復号手段の一実施例を示す構成図である。

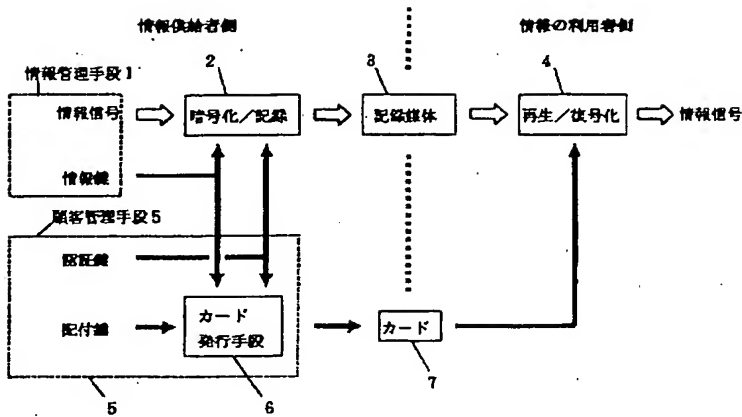
【図6】コード変換器の一実施例を示す構成図である。

【図7】コード変換器での動作の一例を説明するための図である。

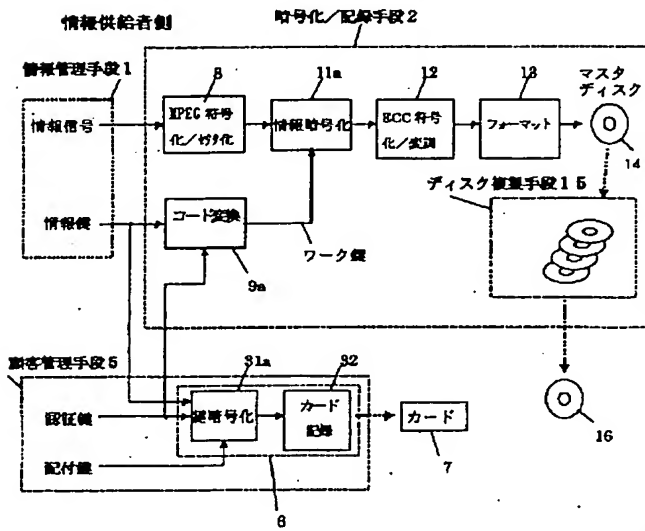
【符号の説明】

- 1 情報管理手段
- 2 暗号化／記録手段
- 3 情報記録媒体
- 4 再生／復号手段
- 5 顧客管理手段
- 6 カード発行手段
- 7 カード（カード状情報記録媒体）
- 8 MPEG符号化／セクタ化手段
- 9a, 9b コード変換器（コード変換手段）
- 11a 情報暗号化手段
- 11b 情報復号手段
- 12 ECC符号化／変調手段
- 13 フォーマット手段
- 14 マスタディスク
- 15 ディスク複製手段
- 16 再生用ディスク
- 17 情報再生手段
- 18 復調／エラー訂正手段
- 19 カード解読手段
- 20 セクタ分離／MPEG復号手段
- 21 除算器
- 22 信号分割手段
- 23 セクタ解読手段
- 24 M系列符号発生器
- 25 信号結合手段
- 26 加算器
- 27 ビット列分割／加算器
- 28 ビットローテーション手段
- 29 ビット列転置手段
- 30 加算器
- 31a 鍵暗号化手段
- 31b 鍵復号手段
- 32 カード記録手段
- 33 配付鍵格納手段

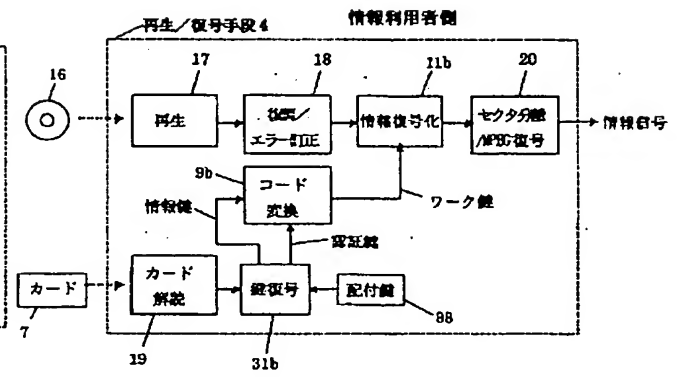
【図1】



【図2】

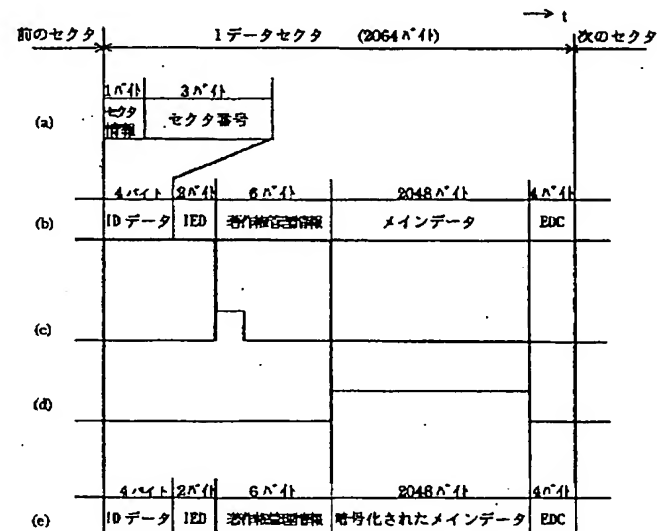
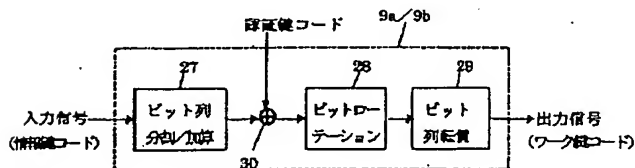


【図3】

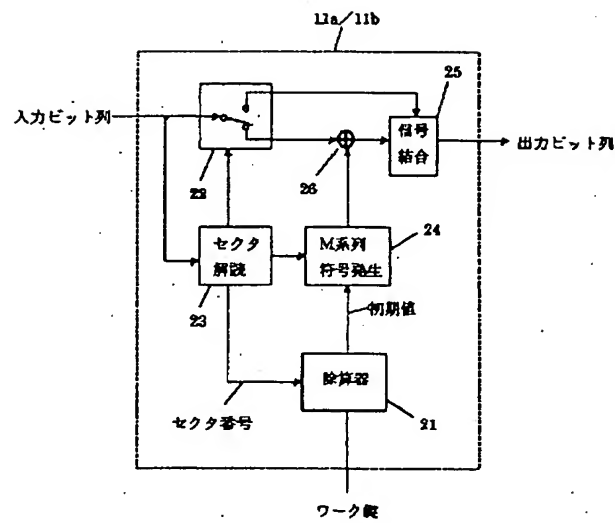


【図4】

【図6】



【図5】



【図7】

